August Ransomware Update

Andy Bennett

Overview

Friday 08/16/19	• **8:36 am:** DIR notified about eight local governments with suspected Sodinokibi ransomware. • **11:00 am:** The number had grown to 19. • **12:00 pm:** Texas SOC at TDEM activated by Gov. Abbott to Level II - Escalated Response Conditions, response directed by Gov. Abbott. • State and Federal incident responders gather at the SOC. • **4:00 pm:** Top three sites identified and support began
Saturday 08/17/19	• **12:00 pm:** Incident responders identify and prioritize all sites by noon.
Sunday 08/18/19	• Incident responders visited all sites by Sunday.
Friday 08/23/19	• All sites are remediated to the point that state support is no longer required.

Overview

- Texas Department of Information Resources (DIR) – Incident Command and Field Incident Response
- Texas Military Department (TMD) – Field Incident Response
- Texas Division of Emergency Management (TDEM) – State Operations Center (SOC) and Logistics Support
- The Texas A&M University System's Security Operations Center/Critical Incident Response Team – Forensics and Field Incident Response
- Private Vendors – Field Incident Response
- Texas Department of Public Safety (DPS) – Image Capture
- Federal Bureau of Investigation – Criminal Investigation
- Department of Homeland Security
- Other State and Federal Partners

Senate Bill 64 (2019)

- A cybersecurity event is included in the definition of a disaster.
- Under Governor orders, the National Guard may assist with defending the state's cyber operations.

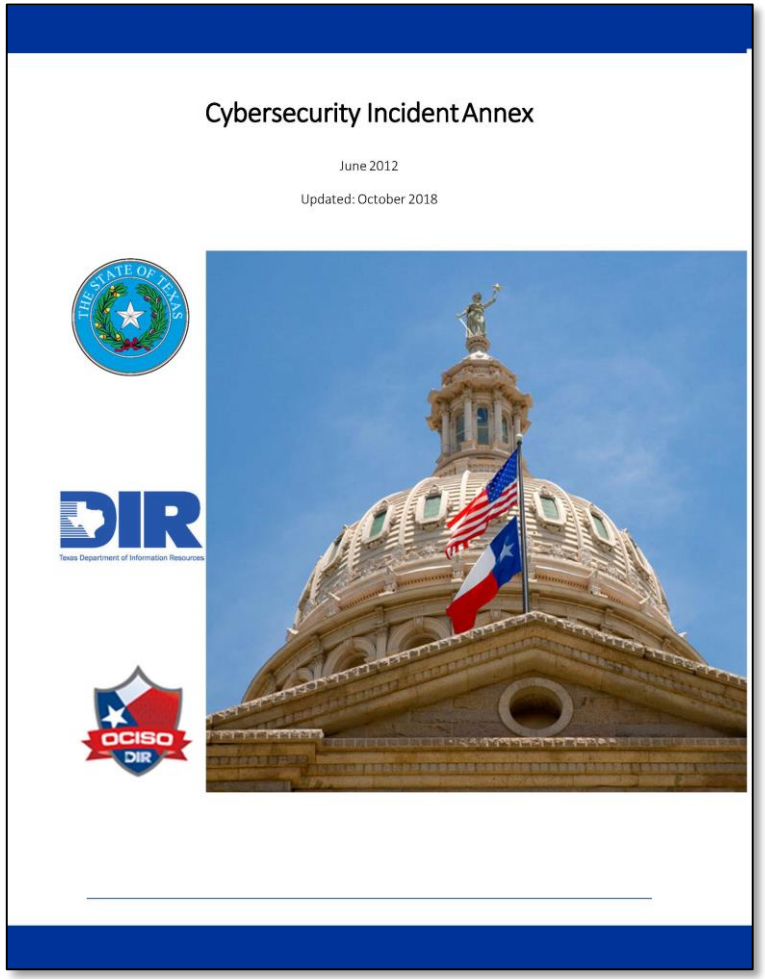
Ransomware Attack Hits 22 Texas Towns, Authorities Say

The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.

The Texas State Capitol and state offices, where the Texas Department of Information Resources is based. The department is leading the response to the cyberattacks. James Leynse/Corbis, via Getty Images

Cybersecurity Annex Development

- House Bill 8 (2017) called for DIR to create a statewide cybersecurity incident response plan.
- The previous TDEM annex had not been updated since 2013 and had not been tested.
- DIR coordinated plan development with TDEM, DPS, and TMD.
- DIR held incident handling training and incident response exercise with partners.



Preparation

Managed Security Services Contract

- Through DIR's Shared Technology Services, local governments can utilize a pre-negotiated cyber incident response contract with a managed security services vendor with no retainer fee.
- All contractors are background checked so they are ready to assist on demand.
- DIR established Service Level Agreements for guaranteed response times.

Eligible Customers

State of Texas Agencies

Local County and City

K-12

Higher Education

Special Districts

Response Activities

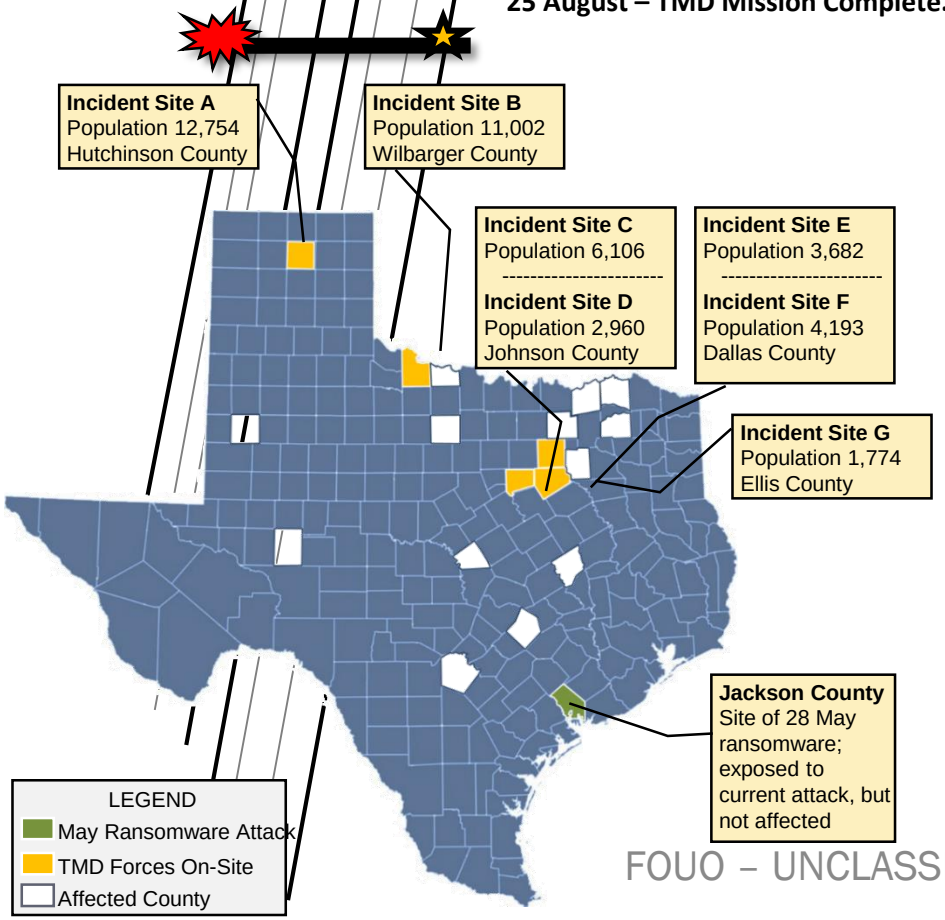
Texas Department of Information Resources (DIR)

- Led and coordinated the state-wide Cyber Incident Response.
- Engaged the Texas Division of Emergency Management (TDEM) to coordinate activities at the State Operations Center.
- Provided direct support for impacted entities.
- Engaged existing MSS contract resources to support local entities.
- Shared information and situational awareness via conference calls and other modes of communication.
- Coordinated the release of public information (press releases from the local governments).
- Coordinated with state and Federal incident response partners including law enforcement (FBI and DPS).

TMD Response Activities

Response Timeline

16 August – Ransomware cyber attack on critical services for 23 Texas entities
16 August – Texas Military Department (TMD) alerted & conducts initial call with state partners and affected entities
16 August – TMD Tasked to provide Cyber Assessment Teams (4 teams of 4 personnel) to three affected municipalities.
17 August - TMD Deploys 4 Cyber teams to 3 affected municipalities
18 August –TMD tasked to deploy 3 additional 8-person Joint Cyber Incident Response Teams
20 August – TMD Redistributes cyber personnel on mission to 2 additional affected municipalities
21-24 August – TMD close out at mission locations, transition to retrograde operations, return to home station.
25 August – TMD Mission Complete.



Mission Summary- The State of Texas conducted a state-wide Cyber Incident Response (IR) mission to address a large-scale ransomware attack that affected more than 23 entities across the state. Texas National Guard deployed seven Joint Cyber incident Response Teams (50+ Personnel) to assist the states response effort. TMD Personnel provided onsite cyber incident response support to seven affected Municipalities, cyber liaison support to the State Operations Center and operational support to the TMD Joint Operations Center.

State & Federal Partners

- **Department of Information Recourses** –Lead Agency
- **FBI**-incident forensic investigation
- **Texas A&M Cyber**-remote cyber assistance
- **Texas Department of Emergency Management**

Response Numbers

- **23** Entities Affected
- **50+** Guard Forces Activated
- **3** Base Security Forces
- **4** Sheriff's Offices
- **7** Police Departments
- **9** Cities & Police Departments

42,471 Texans Served

Response Activities

Texas A&M University System (TAMUS)

- Security Operations Center supported the incident with staff in Austin and working remotely from College Station, TX.
- TAMUS Cyber Response Team (CRT) provided investigative and forensic support.
- Gathered and validated local points of contact and impact information.
- Assisted with tracking status of impacted entities to support resource prioritization.
- Supported communication with both incident responders and impacted entities.
- Coordinated closely with the cyber response teams to support the investigation.

Investigation Report - Summary

On August 16, 2019, a server owned by a managed service provider (MSP) was used to distribute Sodinokibi ransomware to MSP customers. Twenty-three government entities across Texas, with approximately 740 computers, were affected by this attack.

MSP staff contacted a third-party service to assist with negotiating the ransom. After reaching the attackers, the third-party service reported the attackers set the payment at $2.5 million.

Final assessment is that the attacker compromised MSP's ScreenConnect (SC) server. The attacker leveraged the remote software deployment and command execution capability provided by the SC server to execute the ransomware payload on downstream victim workstations and servers. The ransomware deployment part of the attack started on August 16, 2019, at 1:47 AM CDT and ended on August 16, 2019, at 3:25 AM CDT.

Investigation Report – Test Run

- On August 2, 2019 at 7:31 AM CDT, an actor (SODIN23 aka Affiliate 23) gained access to MSP's Screen Connect (SC) server remotely from a Tor exit node.
- The SC software is used by MSP employees to remotely manage their customers' servers and workstations.
- The SC software operates like Microsoft RDP, but also provides the operator with the ability to transfer files and execute scripts or files on client computers that are actively connected to the SC server.
- Between 7:31 and 7:41 AM CDT, SODIN23 used the SC server to remotely connect to a computer in VICTIM1 and the VICTIM2 network attached storage server. The connections were brief.
- SODIN23 was likely testing the ability to connect to other computers remotely and then conducted a brief recon to identify mass storage devices.

Investigation Report

The CRT was not able to confirm the method SODIN23 used to gain initial access to a MSP administrator account on the SC server. CRT analysts reduced it to two scenarios.

Scenario One - SODIN23 acquired the MSP administrator account credentials at some point prior to August 2nd. CRT findings supporting this scenario:

- A brute force attack on the account was ruled out as there were no recent lockouts on any of the accounts, indicating that SODIN23 used valid credentials.
- The session properties in the SC database were consistent with other legitimate sessions where valid credentials are used.
- The MSP administrator account did not have multi-factor authentication (MFA) enabled, so logging in from outside the network was entirely possible using valid credentials.

Scenario Two - SODIN23 exploited a series of vulnerabilities in the SC software to gain access to the MSP administrator account without authentication. Findings:

- Bishop Fox identified several vulnerabilities in the SC software that was running on the MSP server.
- No evidence was found that could support or rule out this scenario.

Investigation Report – Primary Attack

On 08/16/19 at 1:47 AM CDT, SODIN23 returns to the SC server for the primary attack.

At 1:53 AM CDT, SODIN23 used the SC remote execution feature to run a command on one remote computer. We believe this was a test before running the command on all the connected computers. The command executed an encoded PowerShell (PS) script that:

1. Downloaded a second PS script from PasteBin (PB) into process memory.
2. Executed the second PS script in memory creating a new .exe file with the ransomware.
3. Injected the ransomware executable into memory and sleep the PS process for 10 days.

The ransomware would then run in the sleeping PS process and encrypt files. The second PS script to contained code from the pen testing framework “PowerSploit” and the encoded ransomware exe. This is the primary technique used by SODIN23 to deploy ransomware. This technique is effective for evading AV software as it never writes on disk.

Investigation Report – Primary Attack

Roughly one minute after running the command on the first computer, SODIN23 ran “tasklist.exe” to check the running processes.

At 1:59 AM CDT, SODIN23 initiated a task using the SC server to execute the command on all computers connected to the SC server. This task ran for just under a minute when SODIN23 checked the running processes on two other computers.

At 2:39 AM CDT, SODIN23 ran the “dir” command on a victim computer; presumably to check for encrypted files. CRT analysts believe the PS command technique potentially failed to execute the ransomware correctly. CRT analysts identified bugs in the PS code found on PB to support this belief. However, a MSP technician was already responding to the initial customer support call where the ransomware was discovered, so it is possible that the initial deployment was successful. Regardless, SODIN23 decided to initiate the second method of deployment.

Investigation Report – Primary Attack

The “UPDATE.EXE” file first appeared in the “Toolbox” folder on the SC server at 2:41 AM CDT.

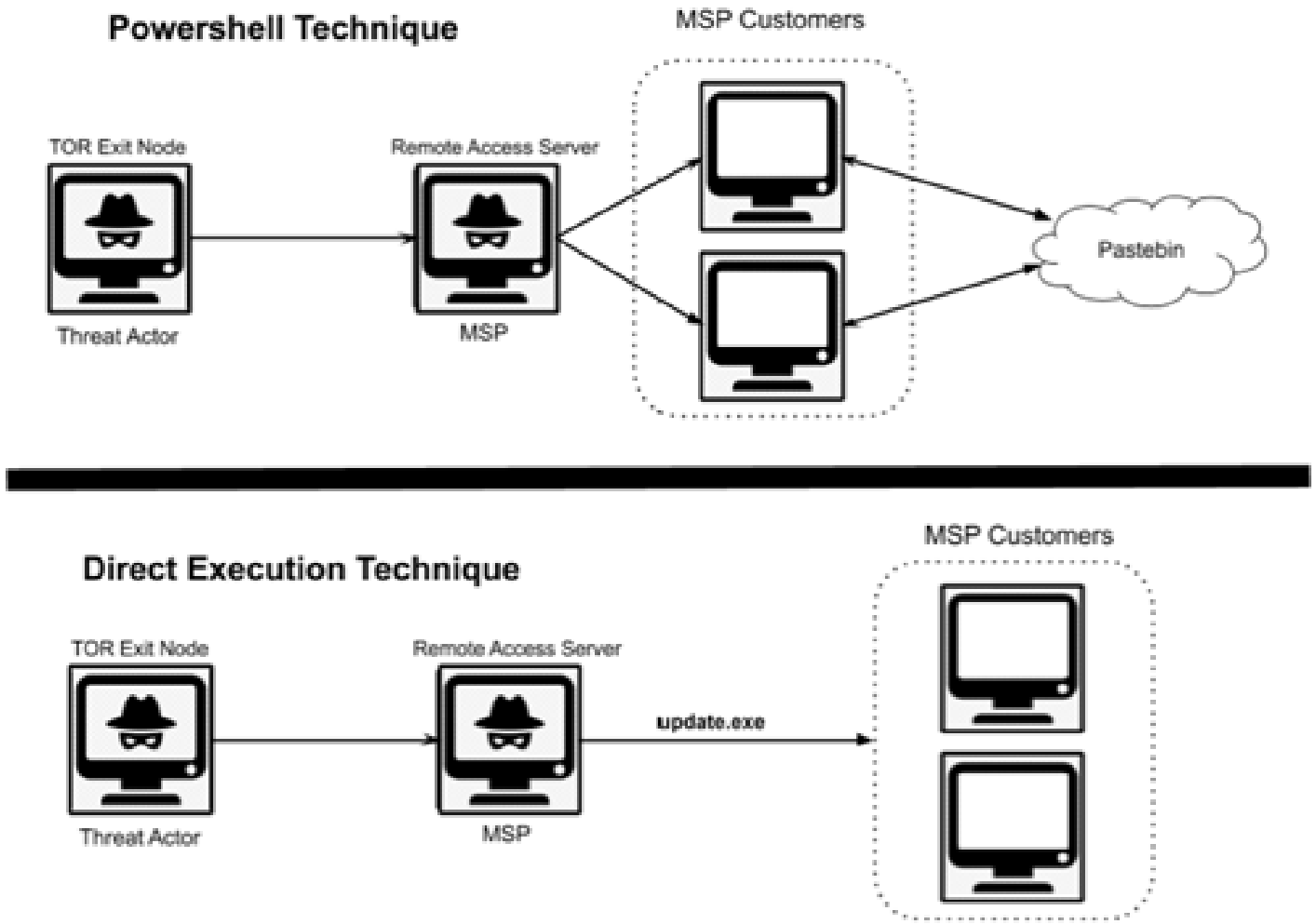
Moments later, the SODIN23 started the second deployment using the SC server, this time using the SC server to copy the “UPDATE.EXE” file to the victim computers and then execute it.

The second deployment ran until approximately 3:25 AM CDT. The ransomware was delivered to the host server that was running the SC server as a virtual machine.

MSP reported that they took the entire host server offline when they noticed files being encrypted on the host server.

The SC server has remained offline since.

Investigation Report – Primary Attack



Key Points and Takeaways

- The single largest factor in the success of this attack was that the ScreenConnect administrator console was exposed to the internet. A management tool with privileged access to a significant amount of endpoints is a very lucrative target for any malicious actor. Exposing it to the internet is extremely dangerous.
- Initial access and recon occurred 14 days prior to the main attack.
- The initial access method was either using valid credentials that were acquired prior to the attack or exploiting a vulnerability chain in the SC software.
- The attack was likely conducted by a single individual who is operating as an affiliate of the Sodinokibi ransomware-as-a-service organization. The Sodinokibi variant used in this attack was configured with “pid: 23”. This is largely thought to be associated with the affiliate’s tenant on the Sodinokibi platform. Thus, we refer to this actor as SODIN23 (FBI refers to it as Affiliate 23).

Key Points and Takeaways

- SODIN23 spent just under an hour and a half conducting the attack. 30 minutes of which was waiting to determine the effectiveness of the attack.
- SODIN23 decided to use a second deployment method either due to questioning the effectiveness of first deployment, or to ensure maximum effectiveness by using two delivery methods.
- SODIN23 appeared to be very familiar with how to operate the ScreenConnect software. We suspect ScreenConnect is part of SODIN23's targeting criteria.
- CRT analysts did not identify any indications of SODIN23 attempting to establish persistence in the MSP environment.
- We recovered 40 distinct Sodinokibi payloads that were uploaded to PasteBin during the month of August. We identified 10 unique affiliate IDs. SODIN23 was the most active affiliate with 12 payloads. This suggests that there were around 10 different affiliates who conducted around 40 attacks using the Sodinokibi platform in August alone.

Indicators of Compromise

Value	Type	Context
a5bdda938b803e1c004d858e127f8ce0	md5	update.exe (Sodinokibi)
4f0069e5575acc9831a89f4e7e903cb94d43db47	sha1	update.exe (Sodinokibi)
df3e960d0f29e9dad6213dccdb5d6ad0a103f40fccb516e56944124f58ab7eeb	sha256	update.exe (Sodinokibi)
23[.]129[.]64[.]210	ip	Attacker IP
77[.]247[.]181[.]165	ip	Attacker IP
23[.]129[.]64[.]182	ip	Attacker IP
46[.]165[.]245[.]154	ip	Attacker IP
23[.]129[.]64[.]152	ip	Attacker IP
185[.]220[.]101[.]7	ip	Attacker IP
81[.]17[.]27[.]138	ip	Attacker IP

Recommendations to Protect from this Type of Attack

The following security practices are recommended to help protect from this type of attack:

- Only allow authentication to RA software from inside MSP's network
- Use two-factor authentication on remote administration tools and VPNs
- Block inbound network traffic from Tor Exit Nodes
- Block outbound network traffic to PasteBin
- Use EDR (Endpoint Detection and Response) to detect PS running from unusual processes

Lessons Learned

- Utilization of the TDEM SOC was a key driver in our success. TDEM is prepared for communicating with the local entities through its district coordinators and has tools (Riot and WebEOC) to communicate with the field teams.
- Triage and prioritization were also important. Knowing which entity to respond to first was critical due to the limited response resources available. Complexity of incident and public safety were used as the criteria.
- Communication protocols to non-impacted entities need to be created.
- The FBI cyber team enabled the Texas A&M cyber team to perform much of the forensics and reverse engineering.
- Through a Texas A&M agreement, DIR was able to deploy end point detection and response software to the impacted entities to detect and prevent any spread or reinfection.
- There is no central designated agency for local entities to report incidents to for the state to perform pattern analysis.

ISF Update

Suzi Hilliard

2020 Information Security Forum (ISF)

- **20th Anniversary**
- **Save the Date:**

  March 10-11, 2020

  Palmer Event Center- Austin, Texas
- **Attendee Registration is open (and almost full)!**

ISF 2020

INFORMATION SECURITY FORUM FOR TEXAS GOVERNMENT

ADJUST YOUR FOCUS

2020 VISION

https://xcelevents.swoogo.com/dirisf2020cfp/395798

All Things ISF

- **Living Security Escape Room**
- **20-minute Vendor Demos**
- **Day Two Focused on Incident Management – don't miss out!**
  - DIR is working with the MSS vendor to provide two tabletop exercises
    - One scenario for local government organizations.
    - One scenario for state level organizations.
  - DHS Incident Management workshop- Assistance with your incident management program
  - ISF Tabletop Panelist Volunteer Opportunity

  Wednesday, March 11, 2020 at 1-3 pm. Use link below to register.

  https://txdir.wufoo.com/forms/isf-tabletop-panelist-volunteer-form/

Developer Training Update

Suzi Hilliard

Proposed Courses

OWASP Requirement	Learning Tree Training Aligned to OWASP Requirements	Key Course Benefits & Real-World Results
1.Injection Attacks 7. Cross-Site Scripting	**Fundamentals of Secure Application Development Course** *2 Days Instructor-Led*	From proactive requirements to coding and testing, this secure software development training course covers best practices any software developer needs to avoid opening up their users, customers and organization to attack at the application layer.
All OWASP Ten Covered	**Secure Coding for Java Course** *3 Days Instructor-Led* **Coding for PHP Course** *3 Days Instructor-Led* **Secure Coding in C Course** *3 Days Instructor-Led*	Courses designed to educate professional programmers on the skills necessary to develop and deploy secure applications. You will learn about potential security issues through concrete, hands-on examples of vulnerable code. Key practical learning from these courses: • Which poor programming practices lead to vulnerable code, how to code securely and how to maintain secure development practices throughout the SDLC. • Sharpen skills and gain experience in applying secure design and implementation principles through demonstrations of building, testing and securing real-world applications. • The opportunity to participate in securing and testing applications through a progression of "challenge scenarios" alternating assignments as "attackers" and "defenders" of applications. ***Common web application exposures and attacks (including those in the OWASP Top Ten).***
OWASP TOP 5	**OWASP Top 10: Risks One Through Five Course** ***On Demand Only** – 215 hours*	This course teaches you the first 5 of the Top 10 in the OWASP list, you will examine: • Injection Attacks • Broken Authentication • Sensitive Data Exposure • XML External Entities (XXE) • Broken Access Control

Proposed Courses

OWASP Requirement	Learning Tree Training Aligned to OWASP Requirements	Key Course Benefits & Real-World Results
OWASP 6-10	**OWASP Top 10: Risks Six Through Ten Course** *On Demand Only – 168 hours*	This course teaches you the OWASP Top Ten items six through ten, you will examine: • Security Misconfiguration • Cross-Site Scripting (XSS) • Insecure Deserialization • Using Components With Known Vulnerabilities • Insufficient Logging and Monitoring
All OWASP TOP 10 Except For Insecure Deserialization	**Cyber Secure Coder Course** *3 Days* *Course is currently being updated and will be available by June 2020*	This course presents an approach for dealing with security and privacy throughout the entire software development lifecycle. Learn about: • Vulnerabilities that undermine security, and how to identify and remediate them in your own projects • General strategies for dealing with security defects and misconfiguration • How to design software to deal with the human element in security • How to incorporate security into all phases of development
1. Injection Attacks 2. Broken Authentication 3. Sensitive Data Exposure 4. XML External Entities (XXE) *Just covered securing XML using digital signature / Covered in detail in CASE java* 5. Broken Access Control 6. Security isconfiguration 7. Cross-Site Scripting (XSS) 9. Using Components With Known Vulnerabilities *Specifically not covered but SAST and DAST techniques cover it indirectly* 10. Insufficient Logging and Monitoring	**Certified Application Security Engineer (CASE) Course** • *CASE.java 3 Days* • *CASE.net 3 Days*	The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment. The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications.

MFA Update

Jeremy Wilson

MFA Background

- **Budget:** Legislature appropriated $7.5 million for this biennium to implement a statewide MFA program for agencies and higher ed
- **Strategy:** Adaptable or Adoptable, Risk Based Approach
- **RFI:** 30 responses told us that there are other solutions, but they would be cost prohibitive and didn't offer functionality or flexibility above what we have with Forge Rock/TX.GOV
- **TX.GOV:** TX.GOV Infrastructure built on FORGE ROCK provided by Deloitte as part of STS and is hosted in AWS Gov cloud for full redundancy and availability
- **POC:** Conducting POCs with 3 agencies to validate our strategy and solution
- **Contractor:** Hired a contractor will be focused on MFA integration and providing assistance to agencies wishing to onboard

Texas.gov Identity Platform - Objectives and Capabilities

Objectives

Objectives

- Enable wide range of MFA capabilities and strong access controls using single digital identity for Constituents and State employees and Higher Ed. users
- Centralized user portal experience for login and access management
- Provide identity administration (a.k.a. Identity governance) and SSO services
- Improve operational efficiency to reduce costs associated with IAM and MFA

Capabilities

Near-term Capabilities

- Multi-factor Authentication (MFA)
- Single Sign On (SSO)
- Federation
- System terms of use acceptance
- Audit capability for system access
- Identity Gateway

Long-term Capabilities

- Identity Administration
  - Separation of Duties (SoD) rules
  - Delegated administration for agencies to be able to manage their users
- Access request and approval workflows
- Privileged Identity and Access Management*

* - Separate licenses to be procured by consuming agency

Texas.gov MFA Identity Platform Overview

Texas.gov Identity Platform (IDP) has been built to support Identity as a Service (IDaaS) architecture. We are currently working on a POC with a large, medium, and small agency to validate our solution.

This provides DIR with:

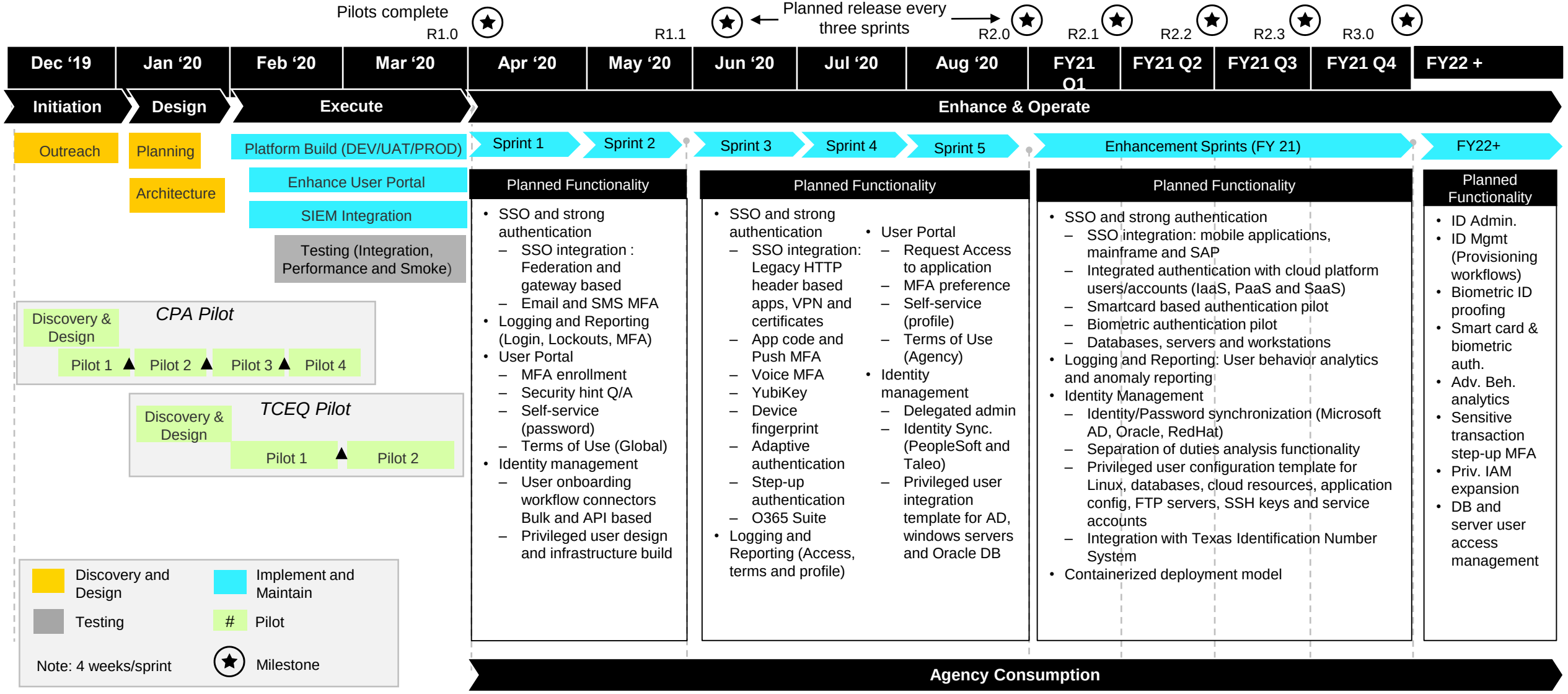
- A centralized platform to provide State agencies and organizations with identity services in a secure and scalable manner
- Multi-tenant, shared services model, by exposing IAM services through RESTful APIs and industry standard protocols such as OAuth2.0, OpenID Connect, SAML and others
- Core Enterprise MFA capabilities
  - Intelligent Authentication, Single Sign-On, Session Management
  - Multi-factor Authentication, Device fingerprinting
  - User Self-Registration, Self-Service
  - User Repository, Password Policies
  - Analytics, Reporting
- Flexible solution to support custom requirements of DIR customers
- High Availability architecture hosted on **AWS GovCloud**

Authentication Considerations

- Multifactor Authentication factors
  - One Time Password (OTP) over SMS and Email
  - Device Fingerprinting
  - FIDO2 compliant hard tokens like Yubikey*
  - Mobile Authenticator App, Push Authentication
  - OTP over Voice Call (requires additional configuration)
  - Biometrics (requires additional configuration)
- Perform MFA based on risk profile of the business application and user risk score
- Adaptive and Step-up authentication
- Use of Device Fingerprinting to reduce re-authentication requirement and improve user experience
- Additional dedicated IAM infrastructure can be added based on agency request*

* - device/infrastructure to be provided by consuming agency

Timelines


Pilots complete
R1.0
R1.1
Planned release every three sprints
R2.0
R2.1
R2.2
R2.3
R3.0
Dec '19
Jan '20
Feb '20
Mar '20
Apr '20
May '20
Jun '20
Jul '20
Aug '20
FY21 Q1
FY21 Q2
FY21 Q3
FY21 Q4
FY22 +
Initiation
Design
Execute
Enhance & Operate
Outreach
Planning
Architecture
Platform Build (DEV/UAT/PROD)
Enhance User Portal
SIEM Integration
Testing (Integration, Performance and Smoke)
Discovery & Design
CPA Pilot
Pilot 1
Pilot 2
Pilot 3
Pilot 4
Discovery & Design
TCEQ Pilot
Pilot 1
Pilot 2
Sprint 1
Sprint 2
Sprint 3
Sprint 4
Sprint 5
Enhancement Sprints (FY 21)
FY22+
Planned Functionality
• SSO and strong authentication
– SSO integration : Federation and gateway based
– Email and SMS MFA
• Logging and Reporting (Login, Lockouts, MFA)
• User Portal
– MFA enrollment
– Security hint Q/A
– Self-service (password)
– Terms of Use (Global)
• Identity management
– User onboarding workflow connectors Bulk and API based
– Privileged user design and infrastructure build
Planned Functionality
• SSO and strong authentication
– SSO integration: Legacy HTTP header based apps, VPN and certificates
– App code and Push MFA
– Voice MFA
– YubiKey
– Device fingerprint
– Adaptive authentication
– Step-up authentication
– O365 Suite
• Logging and Reporting (Access, terms and profile)
• User Portal
– Request Access to application
– MFA preference
– Self-service (profile)
– Terms of Use (Agency)
• Identity management
– Delegated admin
– Identity Sync. (PeopleSoft and Taleo)
– Privileged user integration template for AD, windows servers and Oracle DB
Planned Functionality
• SSO and strong authentication
– SSO integration: mobile applications, mainframe and SAP
– Integrated authentication with cloud platform users/accounts (IaaS, PaaS and SaaS)
– Smartcard based authentication pilot
– Biometric authentication pilot
– Databases, servers and workstations
• Logging and Reporting: User behavior analytics and anomaly reporting
• Identity Management
– Identity/Password synchronization (Microsoft AD, Oracle, RedHat)
– Separation of duties analysis functionality
– Privileged user configuration template for Linux, databases, cloud resources, application config, FTP servers, SSH keys and service accounts
– Integration with Texas Identification Number System
• Containerized deployment model
Planned Functionality
• ID Admin.
• ID Mgmt (Provisioning workflows)
• Biometric ID proofing
• Smart card & biometric auth.
• Adv. Beh. analytics
• Sensitive transaction step-up MFA
• Priv. IAM expansion
• DB and server user access management
Discovery and Design
Implement and Maintain
Testing
Pilot
Note: 4 weeks/sprint
Milestone
Agency Consumption

DIR Security Operations Update

SecOps January 2020 Summary

- NSOC Perimeter Security

- The NSOC processed 12 alerts for 4 state agencies during the month of January. Half of the alerts this month were for DDoS. The remainder were for Suspicious Activity, Malware and Phishing in descending order.

- The NSOC blocked 1.1 billion malicious communication attempts in January.

- It is significant to note that we are now geo-blocking all communication attempts from Iran, Sudan, Syria, and North Korea. We are also having to block DNS requests from TOR exit nodes.

Active Threats

Fraud/Organized Crime – High Threat: Ransomware/Phishing

Phishing attacks continue to be attack of choice. User awareness is paramount to our defense. Agencies continue to report phish emails but only a few agencies are participating.

We encourage all agencies to forward suspected phishing activity to security-alerts@dir.texas.gov with the suspect e-mail included as an attachment.

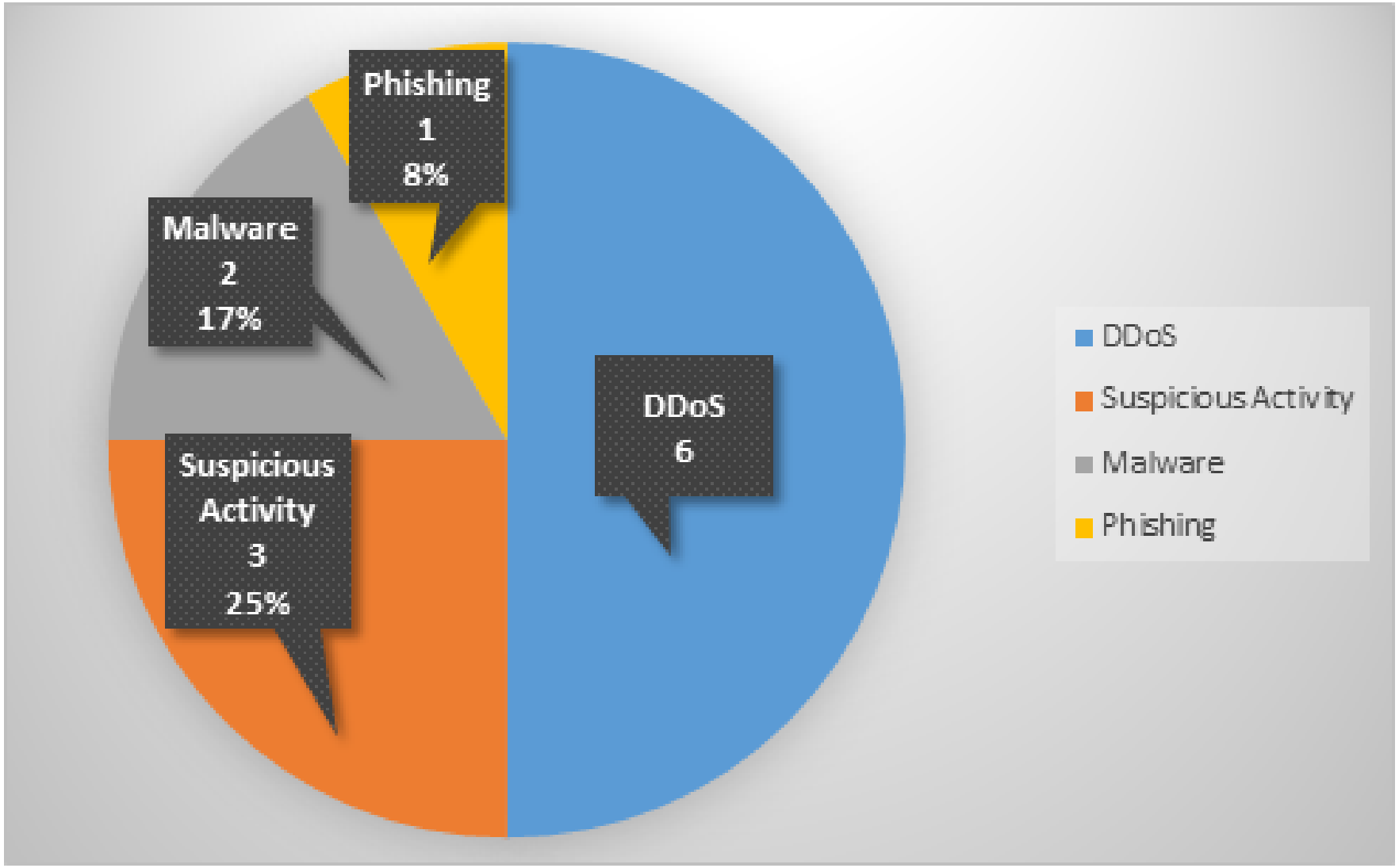
Nation/State –High Threat: Advanced Persistent Threat (APT)

Spear-phishing attacks targeting government employees and contractors continues. APT groups are compromising supply-chain vendors to get to their government targets. They are also exploiting unpatched vulnerabilities on public facing servers to gain entrance into a target network. The NSOC continues to monitor for these activities.

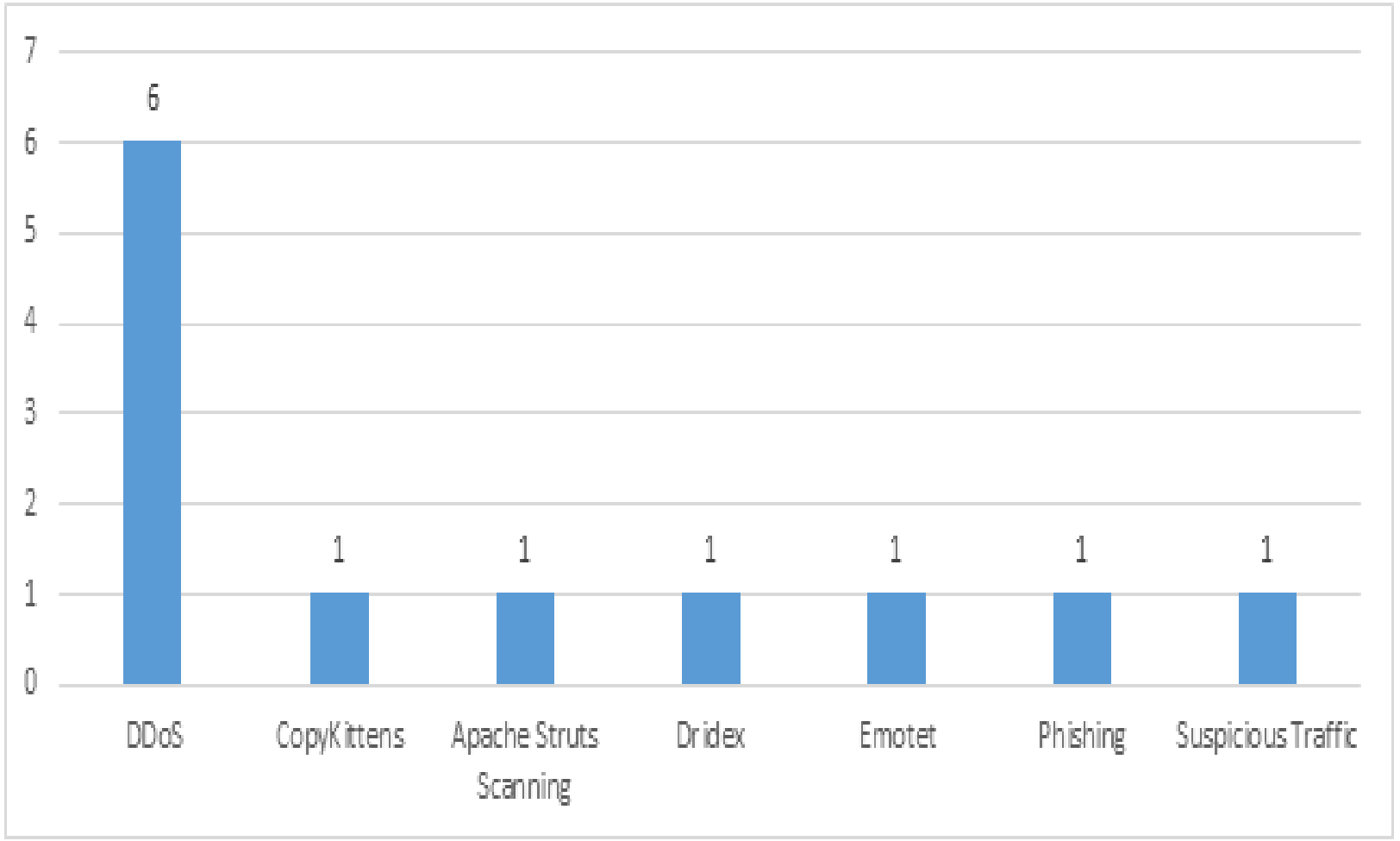
Hacktivists – Low Threat: DDoS/DOX/Web Defacement

We continue to see an increase in short-lived DDoS attacks. Mitigation continues to be successful. We have seen an increase in website defacements. In the past, we have seen pro-Muslim web defacements in the higher education environment. However, in January, pro-Iranian defacements of local and state government websites has been prevalent. Website defacements, while embarrassing, are usually very low impact and low risk to target's networks.

NSOC Alerts January 2020

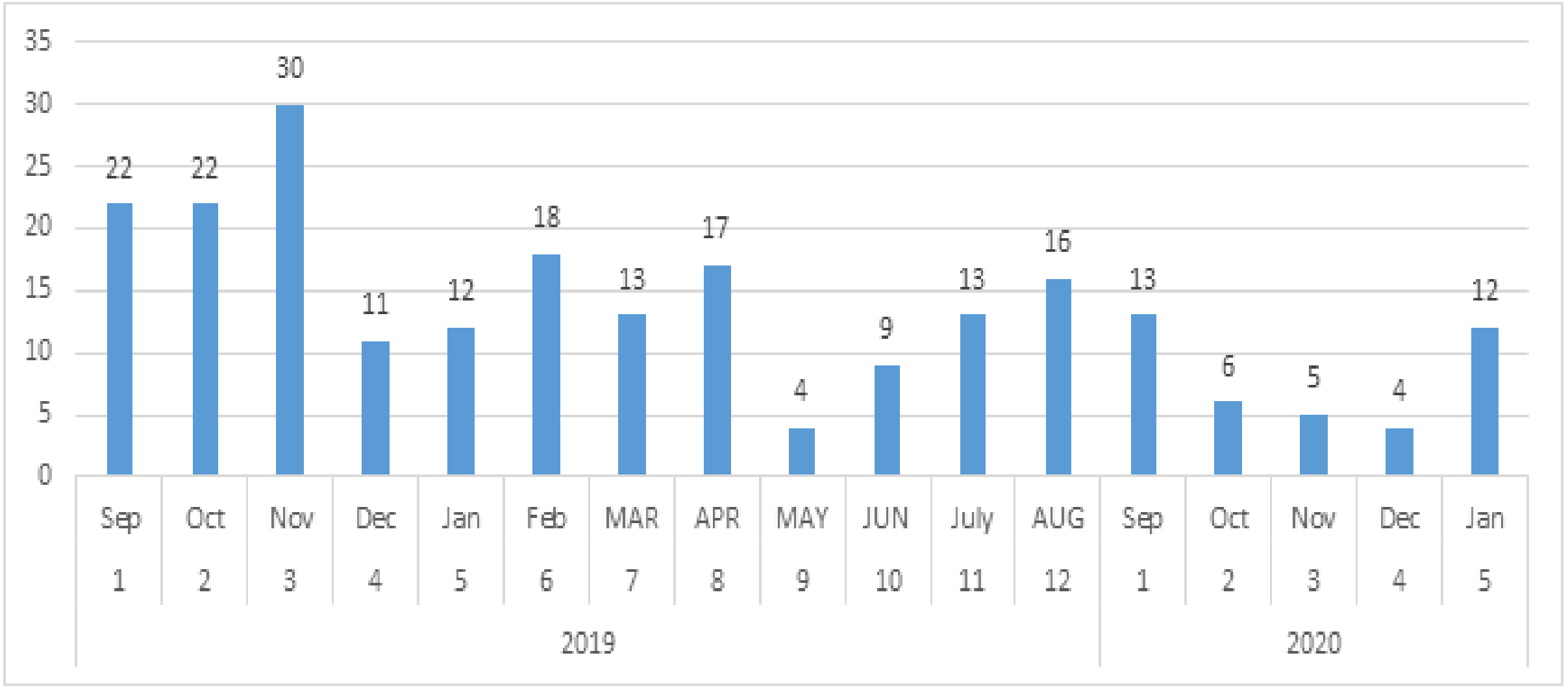


NSOC Alerts by Threat Variant



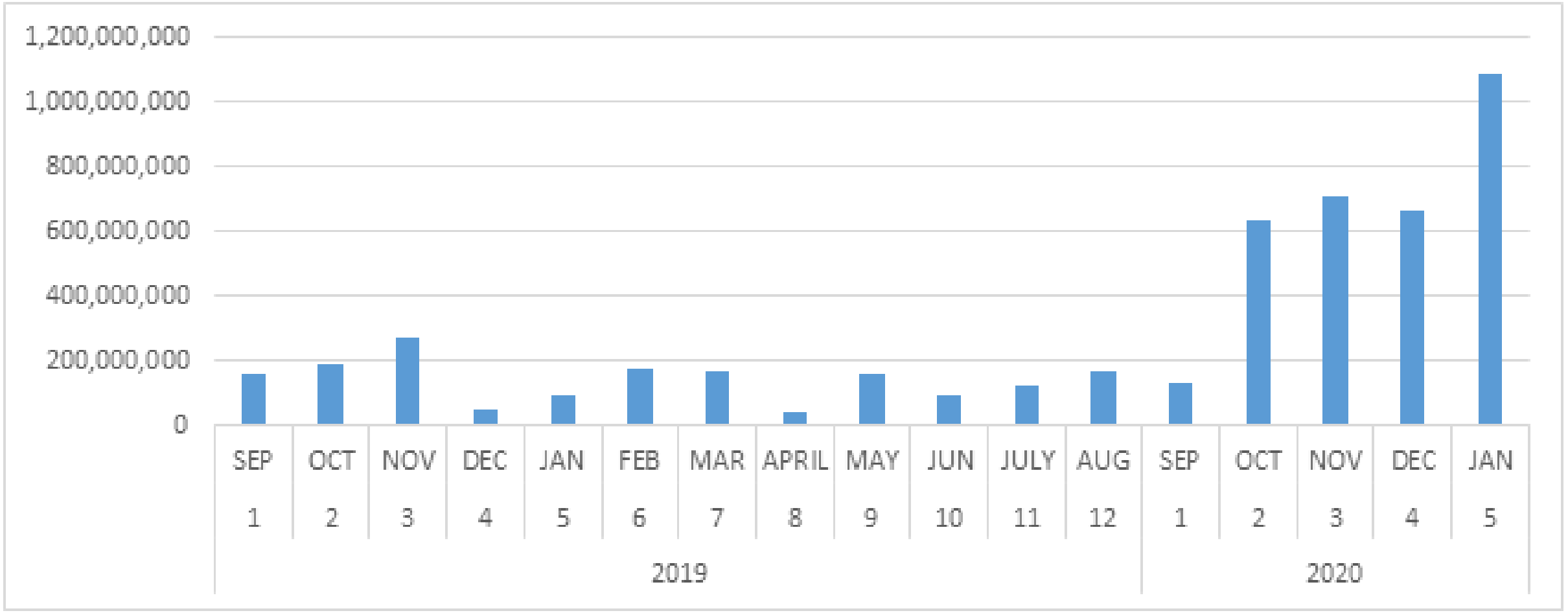
Threat Variant	Alert Count
DDoS	6
CopyKittens	1
Apache Struts Scanning	1
Dridex	1
Emotet	1
Phishing	1
Suspicious Traffic	1
Grand Total	**12**

NSOC Alerts by Month FY19-20

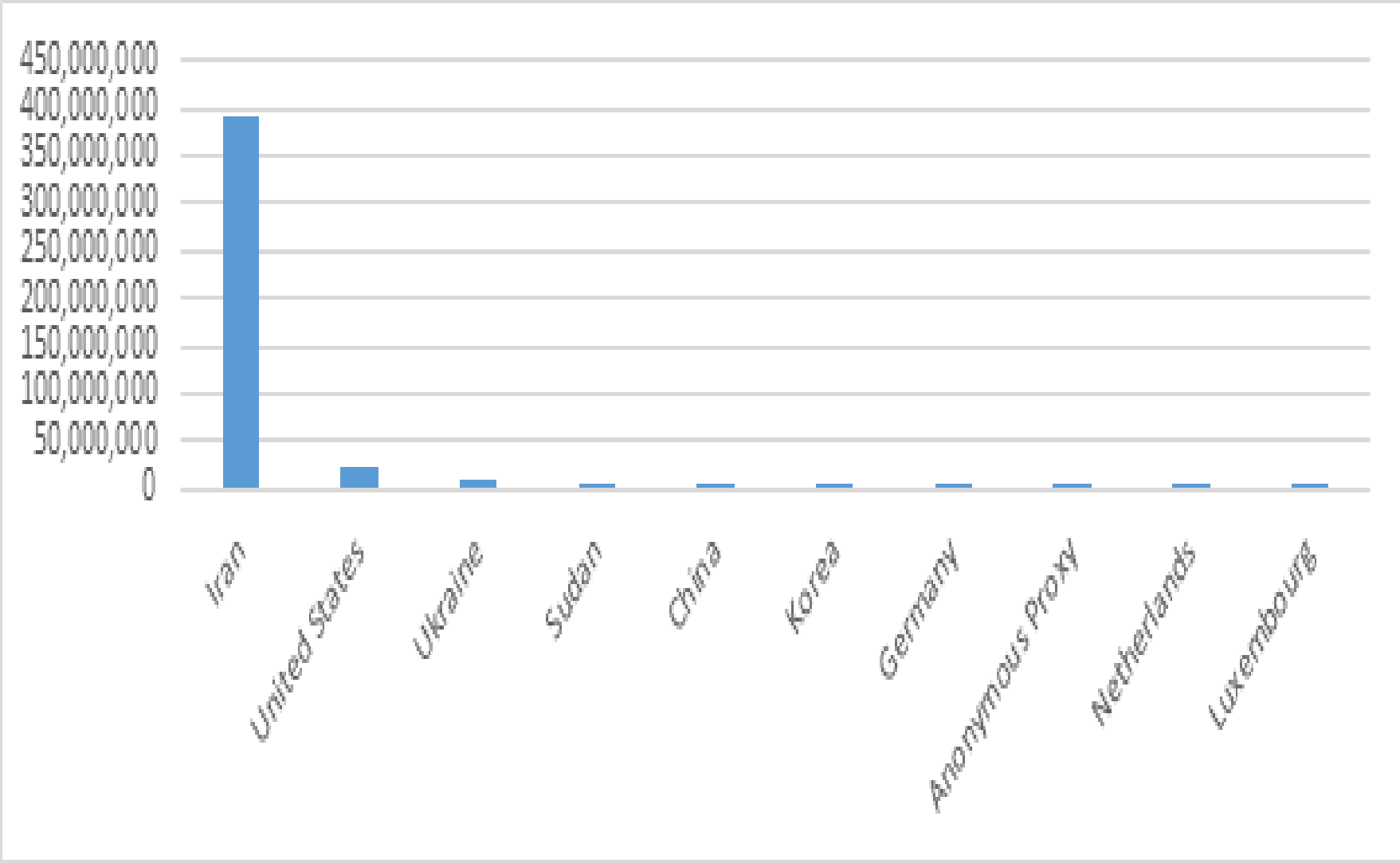


NSOC Logged Blocks FY19-20

The DIR NSOC blocked 1,085,353,903 (1.1 Billion) communication attempts from known bad actors during January 2020.



Top Attacking Countries



Country	Events
Iran	390,707,497
United States	21,369,828
Ukraine	9,359,731
Sudan	5,696,189
China	5,621,866
Korea	3,698,269
Germany	3,570,531
Anonymous Proxy	3,182,890
Netherlands	3,082,866
Luxembourg	2,863,211
Grand Total	**449,152,878**

NSOC Top 20 Most Active Signatures

Signature Filter	Events
Geo Blocked Inbound Iran	352,100,022
Geo Blocked	45,535,733
TOR Exit Nodes	27,846,510
Geo Blocked Inbound Sudan	5,039,251
Geo Blocked Inbound IR KP SD SY	4,418,277
5601: SSH: SSH Login Attempt Client Request	4,118,785
2232: FTP: 'anonymous' User Login	2,842,532
Geo Blocked Inbound Syria	1,903,981
Geo Blocked Outbound Iran	1,365,386
13483: MS-SQL: MSSQL Login Attempt	1,276,946
9982: SMB: Microsoft Windows SMB Server NTLM Lack of Entropy Vulnerability	1,223,285
Geo Blocked Inbound North Korea	447,061
13139: HTTPS: Craigslist Account Login	172,529
Geo Blocked Inbound	168,514
30192: HTTP: zgrab Scanner Detection	151,752
2176: SMB: Null Session SetUp	85,469
5706: SSH: SSH Login Attempt On Non Standard Ports	78,782
22280: HTTP: Joomla Object Injection Vulnerability	73,752
3611: IM: Jabber/Google Talk Client Login Request	68,801
36288: HTTP: vBulletin widgetConfig Unauthenticated Code Execution Vulnerability	62,920

NSOC Initiatives

- Putting New IPS Units into Production
- Texas ISAO
- John Hopkins University Applied Physics Lab – Automated IoC Exchange
- Real-time forensics at the Data Center
- Send suspected phishing emails as an attachment to Security-Alerts@dir.texas.gov

DIR Security Contact Information

Send phishing emails *as an attachment* to
security-alerts@dir.texas.gov.

24HR DIR Cybersecurity Incident Response and Assistance Hotline
Intended to be used by State and Local governments only.
1-877-DIR-CISO

NSOC Security Contact Information
For quickest response, email security-alerts@dir.texas.gov
After Hours On-Call Analysts
(512) 965-8320 or (512)701-7152
DIR Network Helpdesk
(512) 475-2432, option 2
Make sure noreply@archer.rsa.com and noreply@rsa.com are whitelisted for important NSOC Alerting via SPECTRIM

Round Table/Open Discussion

Texas Department of Information Resources

Thank You!

Next Meeting: April 16 at 9:00 a.m.

dirsecurity@dir.texas.gov

security-alerts@dir.texas.gov

DIR Cybersecurity Incident Response and Assistance Hotline

1-877-DIR-CISO (1-877-347-2476)

Intended to be used by State and Local governments only. The phone is answered 24 hours a day, 7 days a week.